BULL. AUSTRAL. MATH. SOC.
VOL. 19 (1978), 117-124.

02K15
(08A05, 16A48)

Dedekind-finite fields

J.L. Hickman

Let p be a prime and let $(m_k)_{k<\omega}$ be a strictly increasing sequence of positive integers such that $m_0 = 1$ and m_k divides m_{k+1}. A field F is said to be of type $(p, (m_k)_{k<\omega})$ if it is the union of an increasing sequence $(F_k)_{k<\omega}$ of fields such that F_k has p^{m_k} elements. A set X is called "finite" if it has n elements for some nonnegative integer n, and "Dedekind-finite" if every injection $f : X \to X$ is a bijection. If the Axiom of Choice is rejected, then it is relatively consistent to assume the existence of medial (that is, infinite, Dedekind-finite) sets. In this paper it is shown that given any type $(p, (m_k)_{k<\omega})$ as above, it is relatively consistent with the usual axioms of set theory (minus Choice) to assume the existence of a medial field of type $(p, (m_k)_{k<\omega})$. Conversely, it is shown that any medial field must be of type $(p, (m_k)_{k<\omega})$ for some $(p, (m_k)_{k<\omega})$ as above. The paper concludes with a few observations on Dedekind-finite rings. In the first part of the paper, a general knowledge of Fraenkel-Mostowski set theory and of the Jech-Sochor Embedding Theorems is assumed.

We work within Zermelo-Fraenkel set theory, but our methods and results are applicable to any of the normal set theories (for example, VNB) that do not contain any Choice Principles as axioms. We obtain our consistency result by constructing an appropriate permutation model of FM

Received 10 July 1978.

set theory, and then transferring to a ZF model via one of the Jech-Sochor Embedding Theorems. The technique is described in Hickman [1], and the relevant details may all be found in Jech [2].

The ordinals are defined inductively by $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, and generally $\alpha = \{\beta; \beta < \alpha\}$. Finite ordinals are known as (natural) numbers, and "ω" will always denote the first transfinite ordinal.

A set X is said to be finite if for some number n there is an injection $f : X \to n$, and infinite otherwise: X is said to be Dedekind-finite if every injection $f : X \to X$ is a bijection, and Dedekind-infinite otherwise. Clearly every finite set is Dedekind-finite, but the converse can only be proved with the aid of some Choice Principle. An algebraic structure A with carrier A is said to be finite (Dedekind-finite) if A is finite (Dedekind-finite).

A set X is said to be countable if there is some injection $f : X \to \omega$. The following result is particularly useful, and is so well-known that we omit the proof.

RESULT 1. *A set X is Dedekind-finite if and only if each countable subset of it is finite.*

A set that is infinite but Dedekind-finite is known as medial.

Let p be any prime, and let $(m_k)_{k<\omega}$ be any strictly increasing ω-sequence of numbers such that $m_0 = 1$ and m_k divides m_{k+1}. Then the ordered pair $(p, (m_k)_{k<\omega})$ is called a "type", and a field F is said to be of type $(p, (m_k)_{k<\omega})$ if it has a strictly increasing sequence $(F_k)_{k<\omega}$ of subfields F_k such that F_k has p^{m_k} elements and $F = \bigcup\{F_k; k < \omega\}$: here of course F, F_k are the respective carriers of F, F_k. Clearly if F is of type $(p, (m_k)_{k<\omega})$, then F has characteristic p.

RESULT 2. *Let the type $(p, (m_k)_{k<\omega})$ be given. Then it is relatively consistent with the axioms of ZF set theory to assume the existence of a medial field of this type.*

REMARK. Since we are engaged upon the task of constructing a model of

https://doi.org/10.1017/S0004972700008492 Published online by Cambridge University Press

set theory in this proof, we are, strictly speaking, working within the meta-theory, and so are permitted to employ the Axiom of Choice.

Proof. Let the type $(p, (m_k)_{k<\omega})$ be given, and for each k let F_k be a field of p^{m_k} elements. Since m_k divides m_{k+1}, the field F_{k+1} contains a subfield isomorphic to F_k; therefore, by the Axiom of Choice, we may assume that F_k is a subfield of F_{k+1} for each k. Put $F = \cup\{F_k; k < \omega\}$; since the F_k's form a chain under inclusion, it is obvious that field operations can be imposed upon F in such a way as to obtain a field F containing each F_k as a subfield.

Construct in the usual manner a model M of FM set theory, having F as its set of urelemente. Within M let G be the group of all field automorphisms on F, and let J be the subgroup filter generated by all G_B with B a finite subset of F, where for any $X \subseteq F$, G_X is the subgroup of G consisting of all $g \in G$ such that $g(x) = x$ for every $x \in X$. Then the couple (G, J) determine an FM submodel N of M containing F. We wish to show that within N the set F is the carrier of a field, which we shall for the moment denote by "F^o", and that F^o is a medial field of type $(p, (m_k)_{k<\omega})$. We recall from the general theory of FM models that each $g \in G$, which is really a permutation on F, can be extended to an $\in$-automorphism (also denoted by "g") on M, and that for each set S in M, we have S in N if and only if $S \subseteq N$ and $G_B \subseteq G_{\{S\}}$ for some finite subset B of F.

Consider in M the set $S = \{(a, b, c) \in F^3; a+b = c\}$, where of course $+$ is the additive operation of F. Since $F \in N$ and N, being a transitive model of FM set theory, is closed under the normal set theoretic operations, we have $F \subseteq N$ and hence $F^3 \subseteq N$. Thus $S \subseteq N$. Now for each $g \in G$ we have $g((a, b, c)) = (g(a), g(b), g(c)) \in S$ for each $(a, b, c) \in S$: the latter relation holds because g is an F-automorphism, and the former relation holds because g is an $\in$-automorphism on M. Thus $G_\emptyset \subseteq G_{\{S\}}$, and so $S \in N$.

https://doi.org/10.1017/S0004972700008492 Published online by Cambridge University Press

In a similar manner we can show that the set $T = \{(a, b, c) \in F^3;\ ab = c\}$ belongs to N. But of course within N the sets S, T determine a field structure on F, and so with respect to S, T we see that F is the carrier of a field F^o in N. Moreover, from our vantage point in M, we can see that F^o and F are isomorphic - in fact, they are identical -, and so it is clear that within N the field F^o is of type $(p, (m_k)_{k<\omega})$. Henceforth we shall identify F and F^o.

We must now show that F is a medial field within N. Certainly F is infinite in N; for if not, there would exist in N an injection $f : F \to n$ for some number n; and since N is a submodel of M, the same injection would exist in M, contradicting the fact that F is infinite in M.

Thus we must simply show that within N there is no injection $f : \omega \to F$; once this has been done, Result 1 will tell us that F is Dedekind-finite and hence medial in N. Therefore suppose that such an injection f does exist in N. By the criterion for membership in N, we must have $G_B \subseteq G_{\{f\}}$ for some finite subset B of F.

Choose k such that $B \subseteq F_k$; such a number certainly exists because B is finite. On the other hand, since $f : \omega \to F$ is injective, there must exist m and r with $r > k$ and $f(m) \in F_r - F_k$. Now any finite field is normal over any of its proper subfields, and so there exists an F_r-automorphism g such that $g(a) = a$ for all $a \in F_k$ but $g(f(m)) \neq f(m)$. Clearly $g \in G$, and so $g \in G_B$, whence $g(f) = f$. Therefore $(g(m), g(f(m))) = g((m), f(m)) \in f$, and since $f(m) \neq g(f(m))$, we must have $m \neq g(m)$. But a simple inductive argument shows that $g(n) = n$ for every number n. This contradiction shows that no such f can exist in N. Thus F is medial in N.

We now apply the Embedding Theorem to transfer this result from the FM model N to a ZF model. This completes the proof.

RESULT 3. *Let* A *be a finitely generated algebra, with a well-ordered set* Q *of primitive operations, and an arbitrary set* R *of defining relations. If* A *is Dedekind-finite, then it is finite.*

https://doi.org/10.1017/S0004972700008492 Published online by Cambridge University Press

Proof. There is no loss of generality involved in assuming that Q contains the identity operation ι, defined by $\iota(a) = a$, for all $a \in A$. We let $x_0, \ldots, x_n$ be generators for A, and we denote by "<" the given well-ordering of Q. Put $Q^* = Q \cup \{x_0, \ldots, x_n\}$, and extend $<$ to Q^* by setting $x_i < x_j < f$ for all i, j, f with $0 \leq i \leq j \leq n$ and $f \in Q$.

We now define the set W of all words on $x_0, \ldots, x_n$ with respect to Q in the usual manner; each $w \in W$ will be a finite sequence with terms in Q^*; and since Q^* is well-ordered by $<$, we can extend $<$ to a well-ordering of W, which we shall still denote by "<", in the normal lexicographic manner.

We define an equivalence relation $\sim$ on X by letting ∇ be the relational join of all members of R, and setting $w \sim w'$ if $\nabla(w, w')$. Since W is well-ordered by $<$, we can define an injection $h : W/\sim \to W$ by taking, for each $C \in W/\sim$, $h(C)$ to be the $<$-first element of C. Thus $W/\sim$ is either finite or has a countably infinite subset. But clearly $A = W/\sim$ (or there is a bijection $g : A \to W/\sim$, depending upon exactly how the term "algebra" is defined): hence A is finite or else has a countably infinite subset. Therefore, if A is Dedekind-finite, then by Result 1 it must be finite.

RESULT 4. *Let F be a medial field. Then there is a type $(p, (m_k)_{k<\omega})$ such that F is of this type.*

Proof. Let 0_F, 1_F be the zero and unit respectively, and for each number m, let m_F be the F-sum $1_F + 1_F + \ldots + 1_F$ having m summands. Then $\{m_F \in F; m < \omega\}$ is a countable subset of F and hence finite, from which it follows that $m_F = 0_F$ for some $m > 0$. It is routine to show that the least such m is a prime, which we shall call "p", and that F has characteristic p. We commence our sequences by putting $m_0 = 1$ and $F_0 = \{k_F; k < p\}$. Obviously F_0 is the carrier of a subfield F_0 of F.

In a similar fashion, we can show that for each $a \in F^* = F - \{0_F\}$

https://doi.org/10.1017/S0004972700008492 Published online by Cambridge University Press

we have $a^m = 1_F$ for some $m > 0$, and we denote the least such m by "$o(a)$". The set $\{o(a);\ a \in F^*\}$ is an unbounded set of numbers. For if n is any positive number, the set $\{a \in F^*;\ o(a) \leq n\}$ is finite, since it is the set of F-roots of the finite equation-set $\{x^j = 1;\ 1 \leq j \leq n\}$.

Suppose that m_k and F_k have been defined, and put $n = \max\{o(a);\ a \in F_k^*\}$. This maximum certainly exists, because F_k^* is finite. We have just seen that $o(b) > n$ for some $b \in F^*$, and so we can define r_k to be $\min\{o(a);\ a \in F^* \ \&\ o(a) > n\}$. Now put $X = \{a \in F^*;\ o(a) \leq r_k\}$; then $F_k^* \subsetneq X$ by our choice of r_k. However, the equations argument shows that X is finite, and so the subfield F_{k+1} of F generated by X is also finite, by Result 3. As a subfield of F, this field F_{k+1} must have characteristic p, and therefore has $p^{m_{k+1}}$ elements for some well-defined number m_{k+1}. Since $F_k \subsetneq F_{k+1}$, F_k is a proper subfield of F_{k+1}, and so m_k is a proper divisor of m_{k+1}.

We observe that our construction process has yielded an auxiliary sequence $(r_k)_{k<\omega}$ of numbers with the property that F_{k+1} contains all $a \in F^*$ such that $o(a) \leq r_k$. Now F_{k+1} is a finite field with $p^{m_{k+1}}$ elements, and the multiplicative group of a finite field is cyclic. Thus there exists $a \in F_{k+1}^*$ with $o(a) = p^{m_{k+1}} - 1$. But by construction, $r_{k+1} > o(a)$ for every $a \in F_{k+1}^*$. This shows that for each $k > 0$, we have $r_k \geq p^{m_k}$, and as $(m_k)_{k<\omega}$ is a strictly increasing sequence, it follows that for any n we have $r_k > n$ for some k. Now we have seen that $o(a)$ exists for each $a \in F^*$; thus if we take any $a \in F^*$ we can choose k such that $r_k > o(a)$, whence $a \in F_{k+1}$. Thus $F = \cup\{F_k;\ k < \omega\}$, and our proof is complete.

It is not true that the type of a medial field determines it up to isomorphism: given any type, it is not difficult to construct a model of

https://doi.org/10.1017/S0004972700008492 Published online by Cambridge University Press

set theory containing two medial fields of that type but of different cardinalities, and hence certainly non-isomorphic. A more interesting question is whether it is possible to have two non-isomorphic medial fields of the same cardinality and type.

We conclude this paper with two short results on Dedekind-finite rings.

RESULT 5. *Every Dedekind-finite division ring is a field.*

Proof. Let $\mathcal{D}$ be a Dedekind-finite division ring, and take any $a, b \in D$. Consider the sub division ring $\mathcal{D}^\circ$ generated by $\{a, b\}$. By Result 3, $\mathcal{D}^\circ$ is finite. But every finite division ring is a field, and so $ab = ba$. Since a, b were chosen arbitrarily, it follows that $\mathcal{D}$ is a field.

RESULT 6. *Every medial ring with only a finite number of zero-divisors is a field.*

Proof. Firstly we consider any infinite ring R whose set Z° of zero-divisors is finite. We shall show that $Z^\circ = \emptyset$. To demonstrate this, we assume that $Z^\circ \neq \emptyset$, and put $Z = Z^\circ \cup \{0\}$, where we are taking 0 as the zero of R. Take any $a \in R - Z$ and define the function f_a with domain Z by $f_a(z) = az$. Clearly $f_a(z) \in Z$ for all $z \in Z$, and so we have defined a function $h : R\text{-}Z \in Z^Z$ given by $h(a) = f_a$. Since Z is finite whilst R is infinite, it follows that $h(a) = h(b)$ for some distinct $a, b \in R - Z$. Put $c = a - b$. Then $c \neq 0$, but $cz = 0$ for all $z \in Z$. But then we see that $c(z\text{-}z') = 0$ for all $z, z' \in Z$, whence as $c \neq 0$ it must be the case that $z - z' \in Z$. This shows that Z is (the carrier of) an additive subgroup of the additive group of R.

Consider R/Z, with the quotient of course being defined with respect to addition. Since Z is finite, each $C \in R/Z$ is finite. Now define for each $C \in R/Z$, $q(C)$ to be $\{h(a);\ a \in C\}$. We claim that $q(C) \cap q(C') = \emptyset$ for distinct $C, C' \in R/Z$. For if for some $a \in C$, $b \in C'$ we have $h(a) = h(b)$, then $(a\text{-}b)z = 0$ for all $z \in Z$. Since $Z^\circ \neq \emptyset$, we can choose $z \in Z$ with $z \neq 0$, and it follows that $a - b \in Z$. But this contradicts the fact that a, b belong to distinct cosets of Z.

https://doi.org/10.1017/S0004972700008492 Published online by Cambridge University Press

Therefore distinct elements of R/Z give rise to disjoint subsets of Z^Z. Since Z is finite, R/Z must be finite. But each $C \in R/Z$ is finite, and so we arrive at the absurd conclusion that R is finite. Thus $Z^\circ = \emptyset$.

Thus every medial ring with only a finite number of zero-divisors is a division ring, and hence a field by Result 5.

We state without proof that it is relatively consistent with the ZF axioms to assume the existence of a medial ring with an infinite number of zero-divisors and either a finite or an infinite number of invertible elements.

References

[1] J.L. Hickman, "The construction of groups in models of set theory that fail the Axiom of Choice", *Bull. Austral. Math. Soc.* 14 (1976), 199-232.

[2] Thomas J. Jech, *The axiom of choice* (Studies in Logic and the Foundations of Mathematics, 75. North-Holland, Amsterdam, London; American Elsevier, New York; 1973).

[3] Serge Lang, *Algebra* (Addison-Wesley, Reading, Massachusetts, 1965).

Department of Mathematics.
Institute of Advanced Studies.
Australian National University.
Canberra.
ACT.